The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)

Project is a collaboration between several UK Universities

The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)

Project is a collaboration between several UK Universities

The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)

Project is a collaboration between several UK Universities

- Concept of a Darknet will be familiar to many

The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)

Project is a collaboration between several UK Universities

- Concept of a Darknet will be familiar to many
- Address space assigned to yourselves that is unused

The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)
Project is a collaboration between several UK Universities

- Concept of a Darknet will be familiar to many
- Address space assigned to yourselves that is unused
- Can be used to detect various forms of malicious traffic

However...

- Per site/organisation Darknet usage brings benefits

However...

- Per site/organisation Darknet usage brings benefits

However...

- Per site/organisation Darknet usage brings benefits

However...

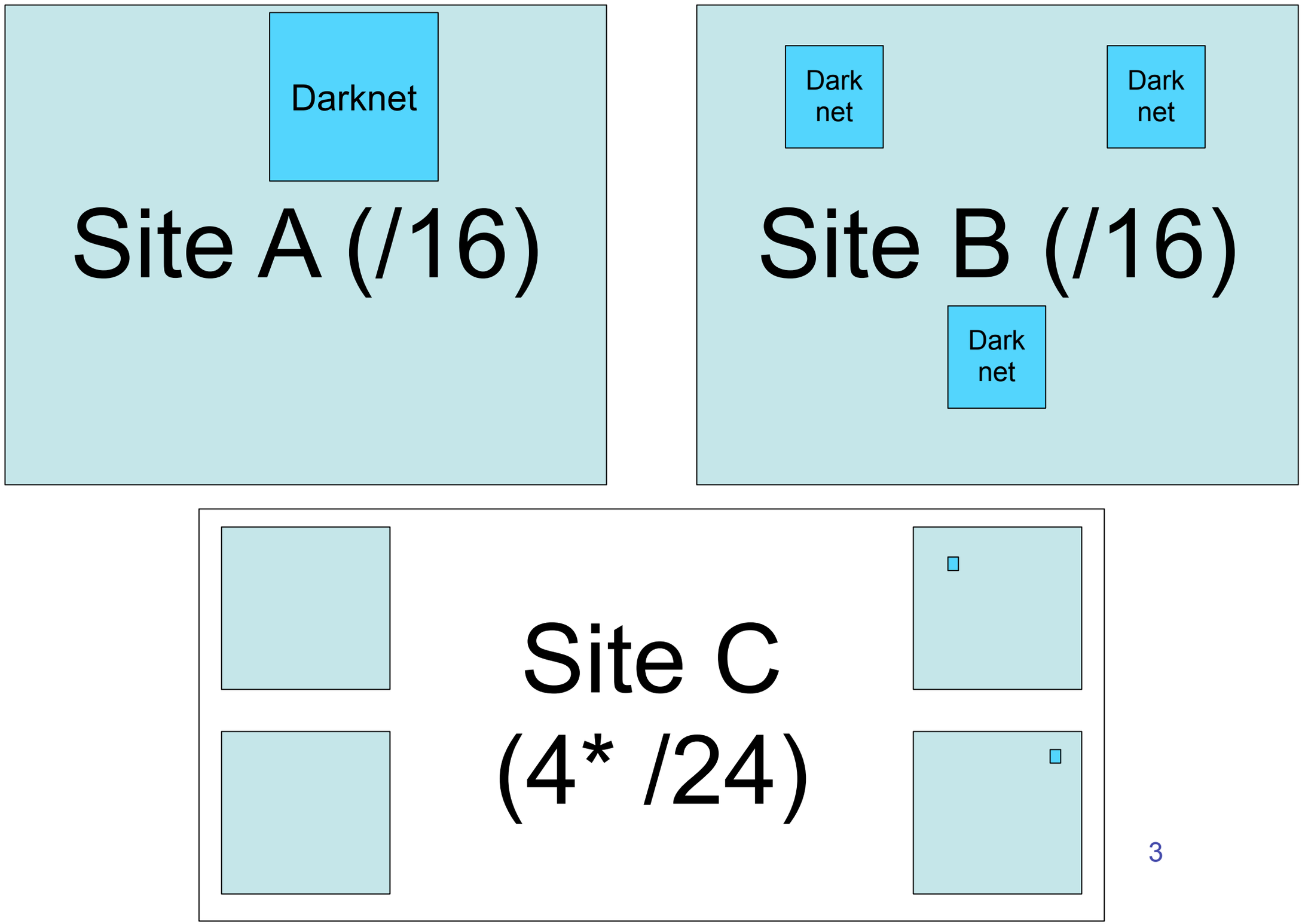
- IPv4 Exhaustion makes obtaining “virgin” IP Space Hard

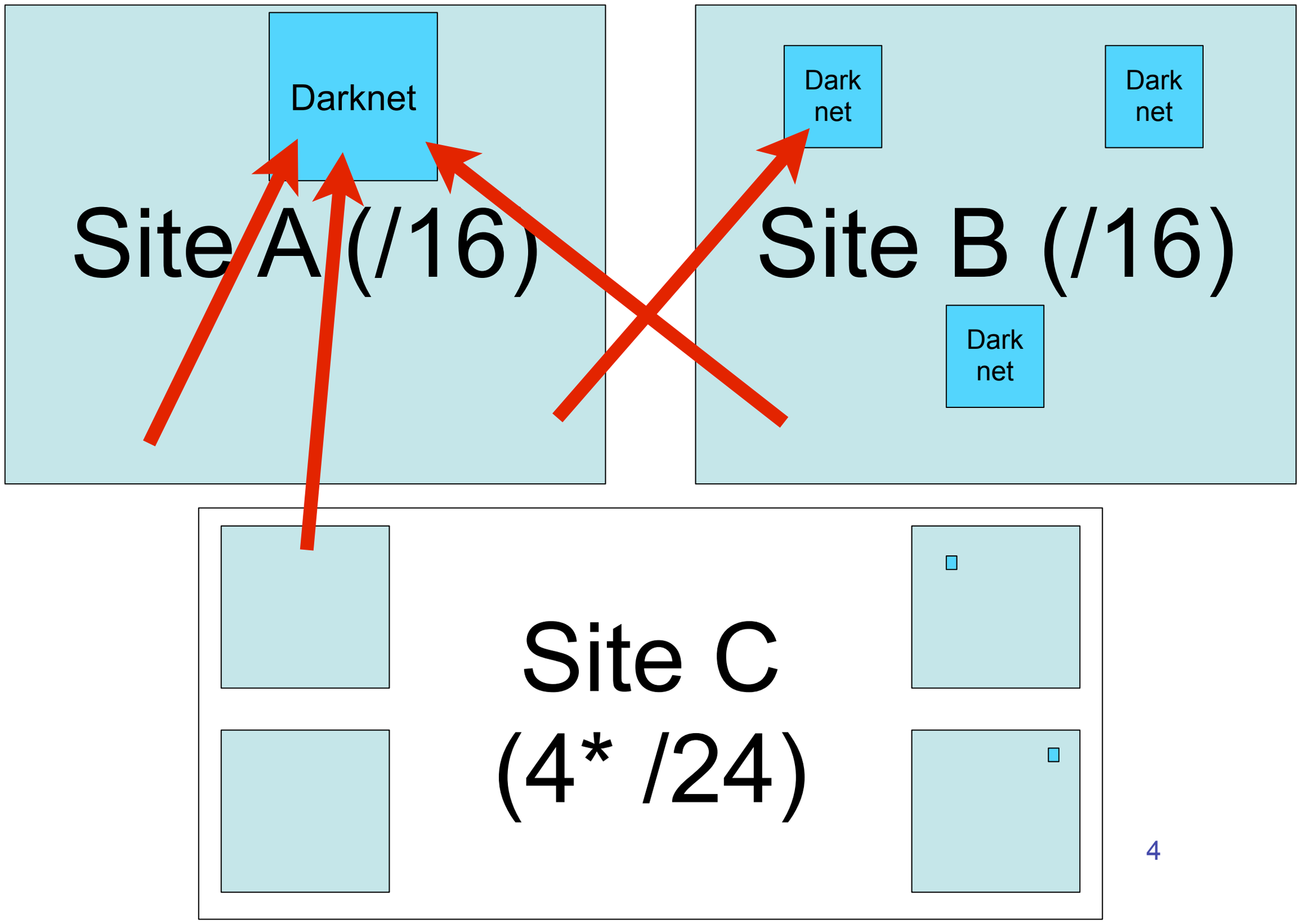
- Per site/organisation Darknet usage brings benefits

However...

- IPv4 Exhaustion makes obtaining “virgin” IP Space Hard
- Scanners tend not to confine themselves to your IP space any more - random scanning more likely than systematic

Example (not to scale)




Darknet
Site A (/16)
Dark net
Dark net
Site B (/16)
Dark net
Site C
(4* /24)

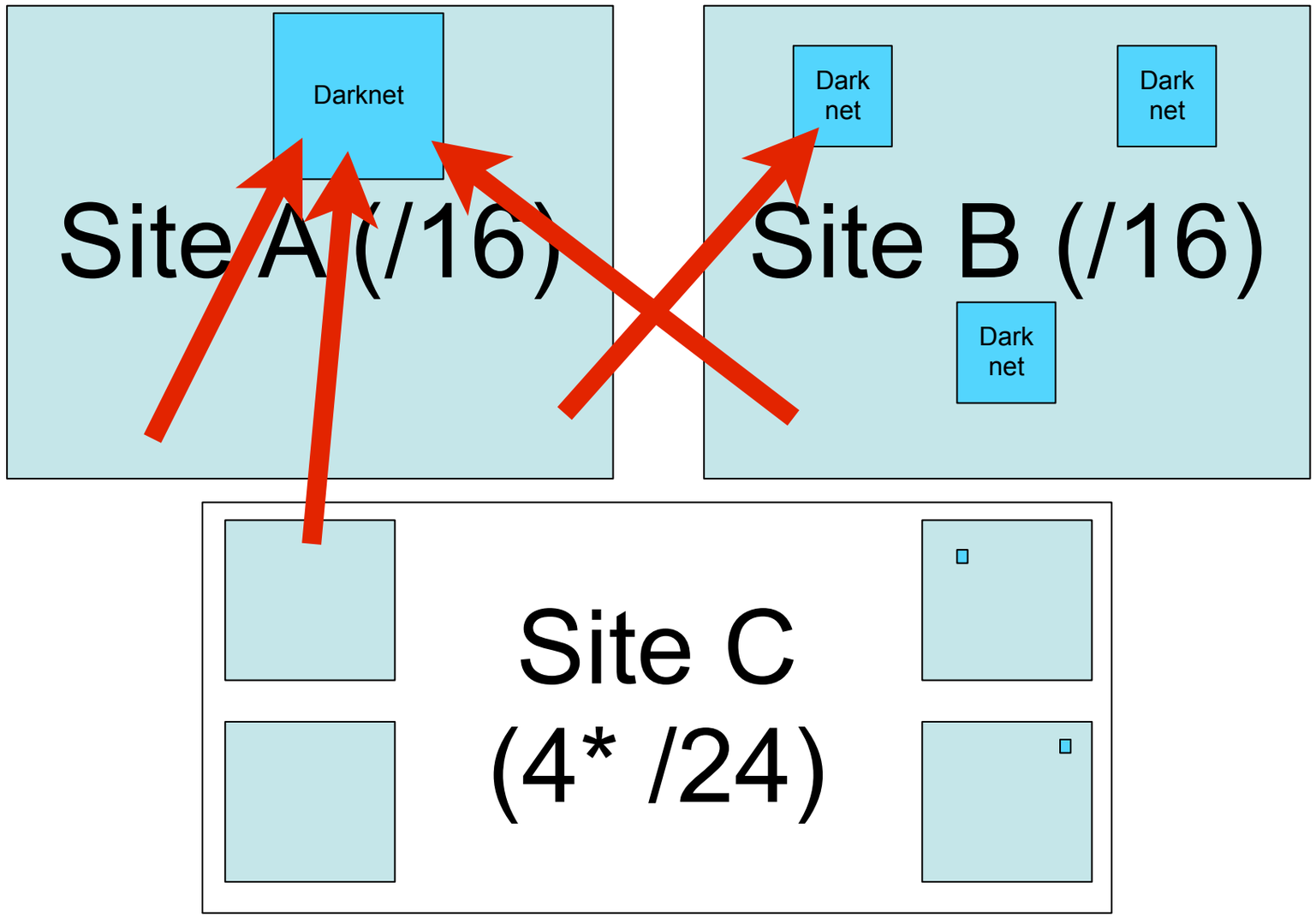
Oxford University Computing Services

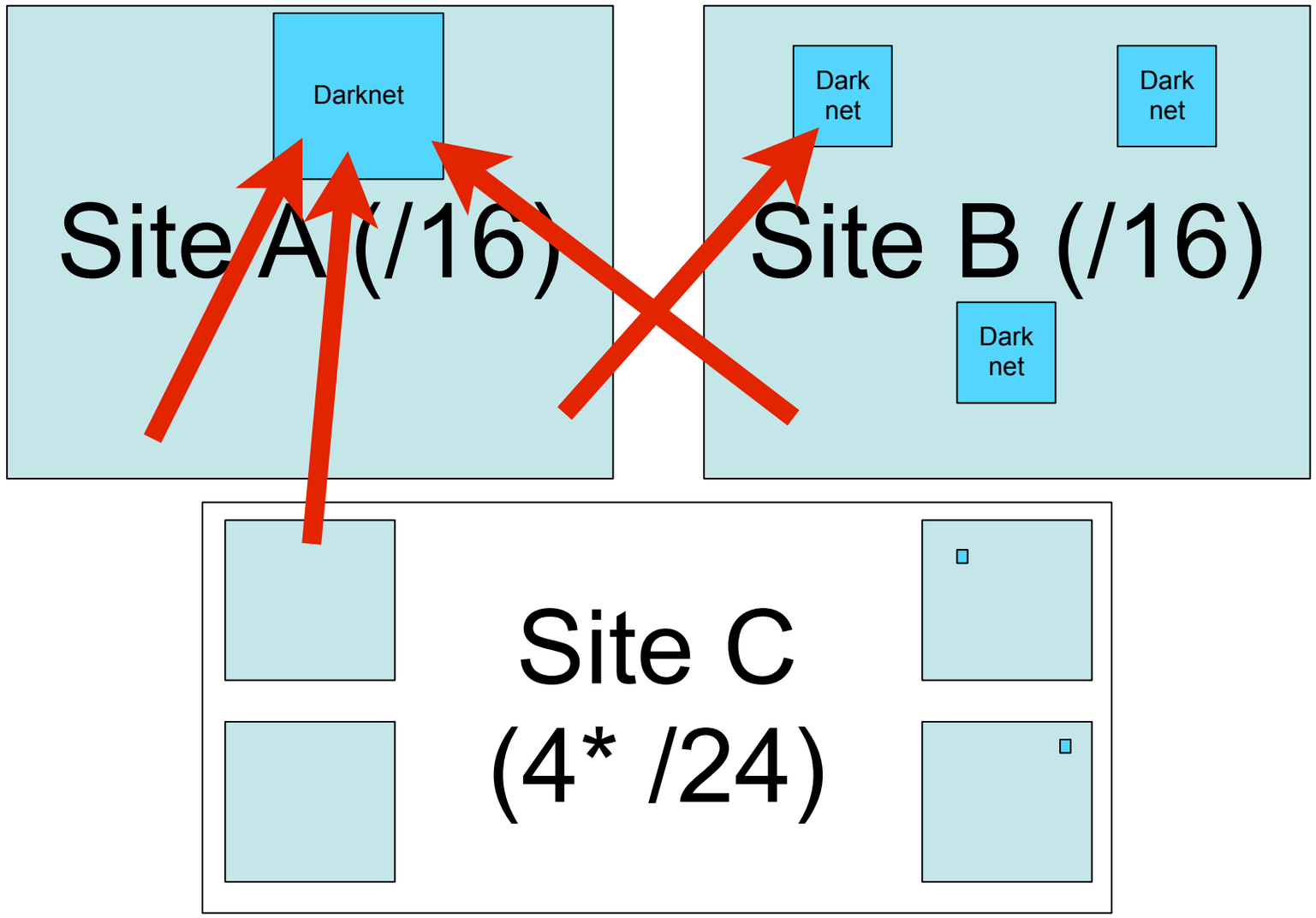
- With a conventional darknet setup, Site A would detect the traffic

- With a conventional darknet setup, Site A would detect the traffic
- Sites B and C might continue in blissful ignorance of a problem

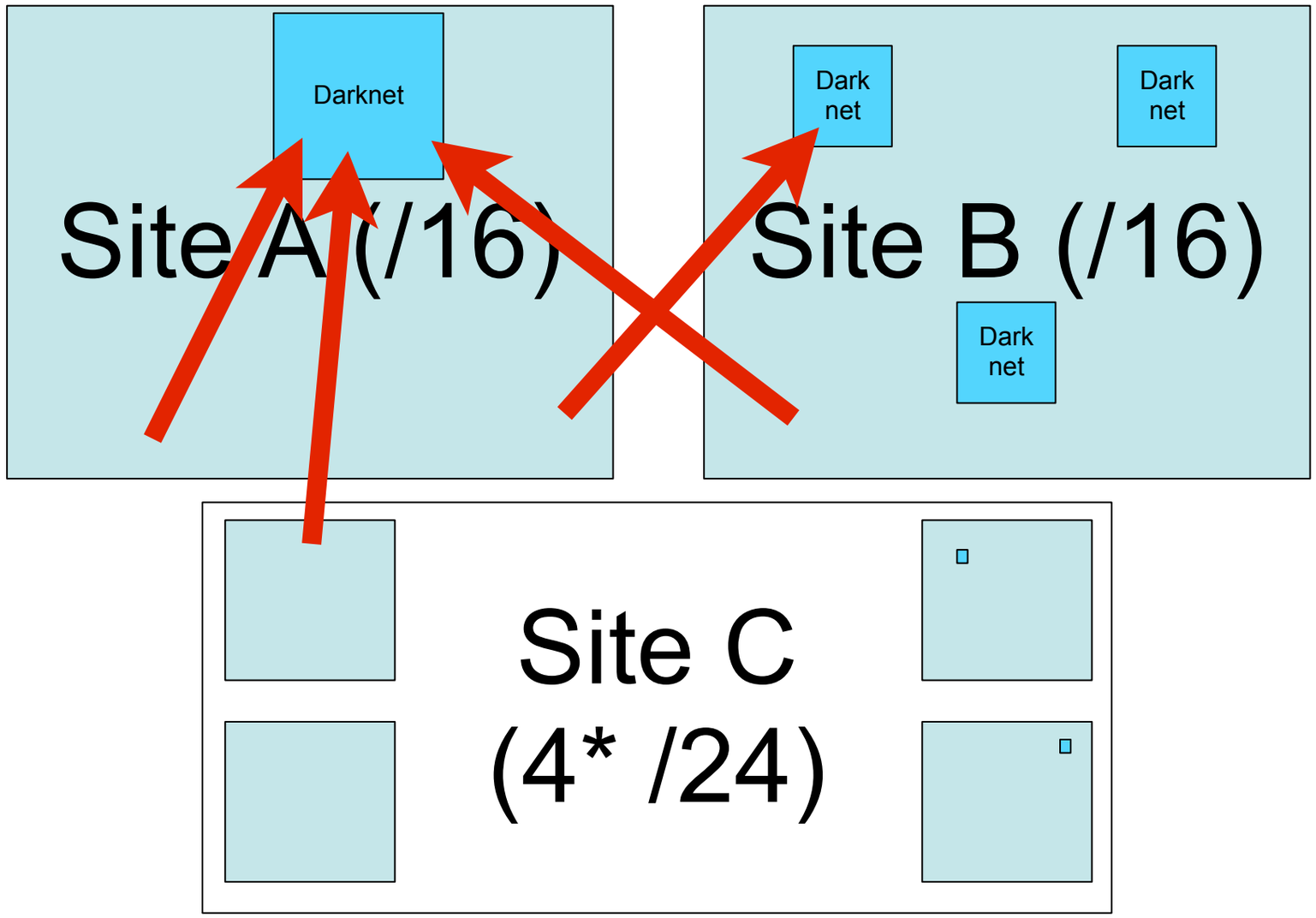
- With a conventional darknet setup, Site A would detect the traffic
- Sites B and C might continue in blissful ignorance of a problem
- Some other solutions exist eg. centralisation of reporting - this requires a lot of work and provides a single point of failure

- With a conventional darknet setup, Site A would detect the traffic
- Sites B and C might continue in blissful ignorance of a problem
- Some other solutions exist eg. centralisation of reporting - this requires a lot of work and provides a single point of failure
- Our approach is to centralise only the registry of netblocks and contacts (and to have a failover if the update is unavailable)


Darknet
Site A (/16)
Dark net
Dark net
Site B (/16)
Dark net
Site C
(4* /24)



- Each Site knows Sites A, B, C's address ranges and a contact, when the sensor sees traffic it contacts the site contact



- Each Site knows Sites A, B, C's address ranges and a contact, when the sensor sees traffic it contacts the site contact
- notification is near instant to the remote site

Further Work

Further Work

- Under active development, new features coming soon, next release will also be packaged for further OSes

Further Work

- Under active development, new features coming soon, next release will also be packaged for further OSes
- http://projects.oucs.ox.ac.uk/darknet

Further Work

- Under active development, new features coming soon, next release will also be packaged for further OSes
- http://projects.oucs.ox.ac.uk/darknet
- Code is freely available so it is possible to either set up your own mesh, or we would consider hosting a wider mesh than currently